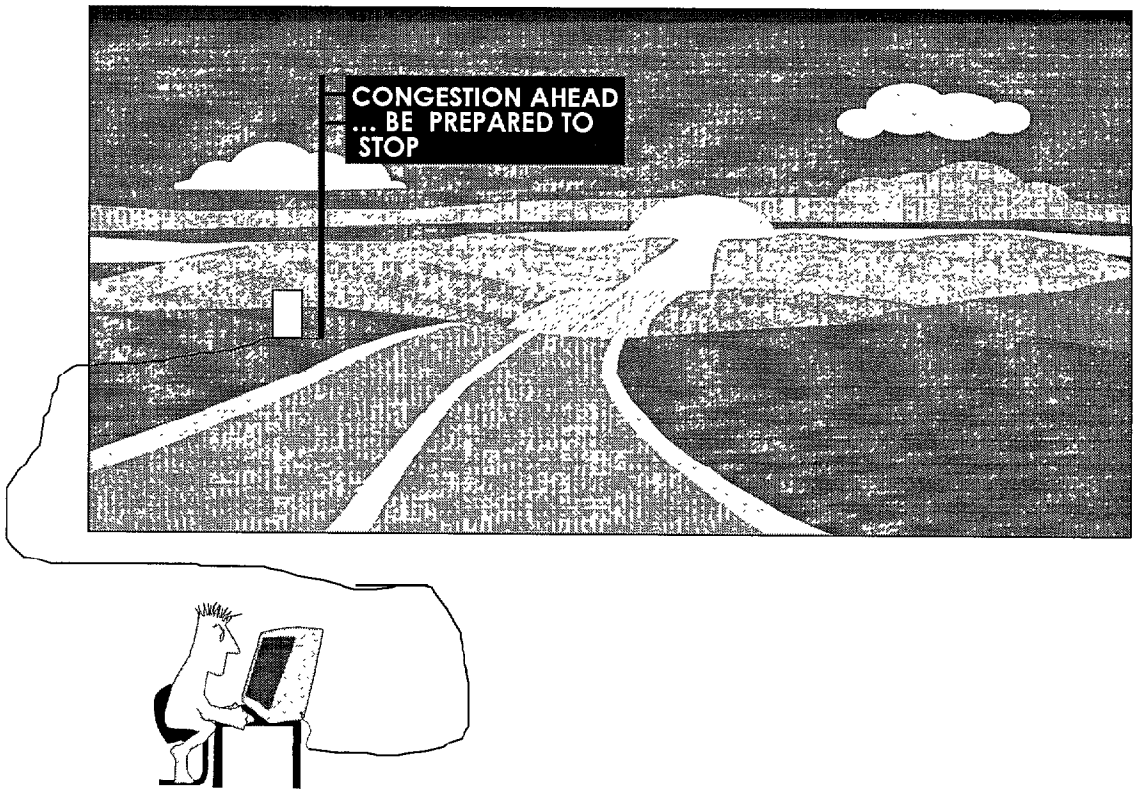
U.S. Department
of Transportation

Protecting Our Transportation Systems:
An Information Security Awareness Overview



Intelligent Transportation Systems
Joint Program Office

150152

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	10/1/1997	Report 10/1/1997

4. TITLE AND SUBTITLE
Protecting Our Transportation Systems: An Information Security Awareness Overview

5. FUNDING NUMBERS

6. AUTHOR(S)
Jones, William S.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Intelligent Transportation Systems Joint Program Office
Washington DC

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

Surface transportation systems increasingly rely on a growing number of sensing, computing, and communications capabilities --collectively known as information technologies. The application of these technologies to our transportation infrastructure has been termed Intelligent Transportation Systems (ITS). Over the past several years, ITS have clearly demonstrated their ability to improve the efficiency of moving goods and people, improve the safety of our transportation system, and provide the public with information on alternative modes of travel.

14. SUBJECT TERMS
IATAC Collection, information security, transportation,

15. NUMBER OF PAGES
24

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

Prepared for the Intelligent Transportation Systems Joint Program Office
by Mitretek Systems

October 1997
Washington, DC

Preface

"The transportation infrastructure has been robust. It has shown great capacity to recover from natural disasters. However, it is more vulnerable now than previously because it is adopting ever larger dependencies on other infrastructure Therefore, it is no longer sufficient to take care of its roads and rails and runways. It must also be concerned with the potential for attacks on ITS installations or on other aspects of telecommunication and computer processing activities that are essential for effective transportation systems."

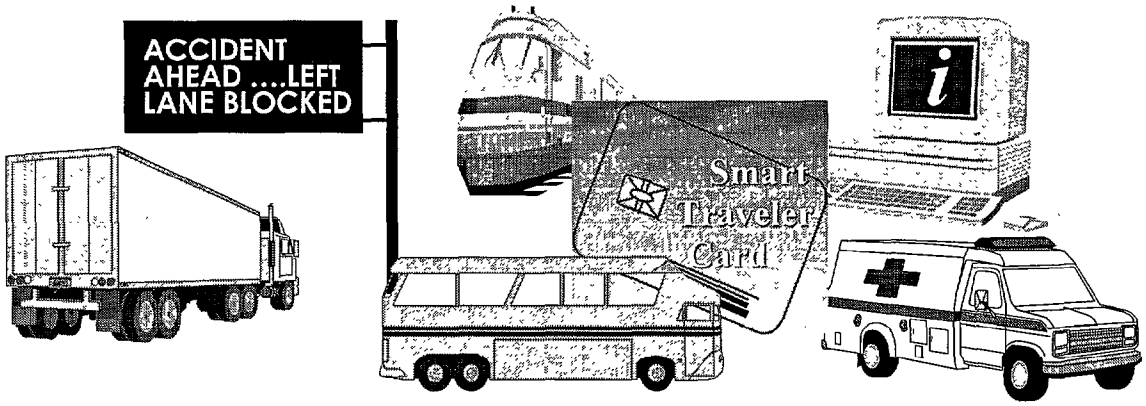
William J. Harris, Commissioner, President's Commission on Critical Infrastructure Protection (PCCIP)

April 1997 briefing to the Board of Directors of the American Association of State Highway and Transportation Officials (AASHTO).

Table of Contents

Introduction

Surface transportation systems increasingly rely on a growing number of sensing, computing, and communications capabilities -- collectively known as information technologies. The application of these technologies to our transportation infrastructure has been termed Intelligent Transportation Systems (ITS). Over the past several years, ITS have clearly demonstrated their ability to improve the efficiency of moving goods and people, improve the safety of our transportation system, and provide the public with information on alternative modes of travel.



Because the application of these information technologies has proven to be cost-effective, they are increasingly deployed by state and local governments. Unfortunately, the threats (i.e., events that can harm the system) and vulnerabilities (i.e., weaknesses in system implementation) affecting these technologies are developing almost as rapidly as the technologies themselves, thus the need for information security.

With the growing reliance on information systems within the global economy, it has become necessary to protect the availability, integrity, and confidentiality of information. Several types of protection -- such as automatic teller machine (ATM) PINs -- have already been integrated into our society and become part of our everyday lives. The military, banking, health-care, and electronic-commerce industries have pioneered this protection effort and have set a precedent for other industries now implementing information systems. As the surface transportation industry enters the information era through the development and deployment of ITS, there is a growing need to apply appropriate information security policies and practices.

Why should I be concerned?

In the most general sense, everyone involved throughout the life-cycle process of ITS should be concerned about information security. While concern may stem from various considerations (e.g., legal, administrative, political, technical, operational), ITS owners, developers, managers, operators, users, and the general public all have vested interests.

The National ITS Program Plan focuses on the development and deployment of interrelated ITS user services (e.g., Travel and Transportation Management services) that are based upon anticipated benefits. These ITS user services will depend upon various transportation information systems. In turn, these systems will rely on a growing number of information technologies -- technologies that may be susceptible to various information security threats.

Because the ITS user services encompass such a wide range of information (e.g., traffic control, safety, financial, personal), they become susceptible to various intentional or accidental threats. The potential impacts of such threats lead to significant concerns regarding public safety and emergency-response effectiveness, corruption of financial transactions, violations of citizen privacy, and the loss of credibility.

Who should be concerned?

Owners -- Individuals or groups who are responsible for information and information systems that process, store, and transmit ITS related information. This includes ITS service providers, either public (e.g., a traffic management center) or private (e.g., a traveler information service provider), and commercial carriers.

Developers -- Individuals or teams involved in procuring, specifying, designing, and/or building ITS information systems (e.g., computers, communications, sensors). This includes software engineers, integration contractors, consultants, security engineers, and communicationengineers.

Managers -- Program and project managers who oversee the design, development, operation, and maintenance of ITS. This includes transportation agency management at federal, state, and local levels, ITS Joint Program Office (JPO) and field program management, ITS service provider management, and liaison management between development and deployment.

Operators -- Individuals or teams that maintain or support the operation of an ITS system. This includes system administrators, network administrators, account administrators, support staff, and maintenance/repair crews (since these individuals deal with system configuration).

Users -- Individuals who use the ITS information systems and the information provided by those systems. This includes consumers (e.g., information service providers, travelers, pedestrians), commercial drivers, and public service workers (e.g., law enforcement, EMS, highway maintenance).

The Public -- Individuals that comprise the general public. This includes pedestrians, travelers, and others who are not necessarily "using" ITS services but who may be directly or indirectly affected by these services.

What could happen?

The following hypothetical, yet realistic, events illustrate potential impacts to various ITS services that result from inadequately secured information.

Travel and Transportation Management user services collect and process information about the surface transportation system, manage various traffic control devices, and disseminate information to travelers. These include a "Traffic Control" user service that manages the movement of traffic on streets and highways.

Hackers Lead Drivers Close to Edge

At the site of a bridge under construction along the new stretch of the Southeast-Southwest Freeway, three motorists were severely injured as the result of an act of vandalism. Apparently, two teenage hackers managed to access the traffic management system computer that is used to control the region's many new electronic-message signs. While toying with the various display messages, the youths unknowingly directed Freeway traffic onto an unfinished entrance ramp of the bridge.

Travel Demand Management user services are designed to increase the use of transportation modes other than the single-occupant vehicle by providing information to travelers prior to their trips. These include a "Pre-Trip Travel Information" service that often processes and retrieves information about a traveler's identity, routing plans, financial transactions, credit identity, and personal interests.

Travelers ' Personal Details Stolen and Sold

A Carport County couple is under investigation for reselling personal information that they illegally obtained from the computer system of a local transportation information service provider (BP). Investigators believe that the couple copied and sold the personal information (e.g., name, date of birth, Social Security Number, credit rating, address) of over 400 customers to prospective businesses in the surrounding area. Apparently the couple, both computer hobbyists, accessed the information by way of the ISP 's World- Wide- Web page (which is accessible to the public). Although the acts clearly violate state computer-theft andprivacy laws, more importantly, they present the possibility of civil litigation against the ISP.

Public Transportation Operations user services are intended to better manage the public transportation system and to provide improved transit information. The "Public Transportation Management" user service automates the operations, planning, and management functions of public transit systems.

Paper Clip Stops Trains!

In southern Slobovia, all trains were halted for approximately an hour because a paper clip fell into the keyboard of the railroad system 's backup traffic control computer. The clip shorted out several keyboard functions causing the computer to continually submit system requests to the main computer. The system ran out of disk space and failed, subsequently, the main computer shut down all trains.

Electronic Payment user services, which will be developed, deployed, and operated by both public and private organizations, support the deployment of many other services, both within and outside the surface transportation domain.

Clerk Charged for Free Rides

A Redmont County woman was arrested last week for illegally using the CrossCounty Expressway. Apparently, the woman, employed as a data-entry clerk at the DMV, was able to access the toll-tag data for the Expressway. Replacing information of legitimate users with the details of her own vehicle, she was able to pass through the Expressway's automated toll-collection facilities.

Emergency Management user services enhance police, fire, and rescue operations by improving the management of and responses to emergency situations. The "Emergency Vehicle Management" user service reduces the time it takes for emergency vehicles to respond to an incident.

Flood of Calls Paralyzes EMS

The city's new centralized emergency management services (EMS) computer system was temporarily locked up as emergency calls flooded the computer processing resources that also (mistakenly) controlled EMS dispatching functions. For approximately 15 minutes, dispatchers could not use the system to communicate with the EMS crews. While the incident was not life-threatening, the route-guidance and incident-response capabilities were severely hampered Had an accident occurred EMS crews might have been delayed or inappropriately equippedfor the emergency situation.

Commercial Vehicle Operations user services reflect the commonality of using advanced information technologies to improve the safety and productivity of the motor carrier industry. Each of these services will require some set of information about the motor carrier, the vehicle, the driver, and occasionally, the cargo. The "Commercial Vehicle Electronic Clearance" user service facilitates domestic and international border clearance.

Heroin Smugglers Impersonate Farmers

Last Tuesday near the Mexican border town of Nogales, Culhala cartel members illegally passed through the new electronic border-crossing checkstation and smuggled nearly 5,000 pounds of heroin into the United States. With help from a legitimate trucking firm, the smugglers were able to forge driver, cargo, and border-clearance information in the truck's computer system and therefore masquerade as legitimate commercial carriers.

Advanced Vehicle Control and Safety Systems user services, in the near term, are characterized by reliance on self-contained systems within a vehicle. The operation of these services can be enhanced by supplementing on-board capabilities with additional sensors deployed in the infrastructure.

Militia's Jam Session Causes Pile-Up

A local militia was found responsible for last month 's 8-car traffic accident along the state's new automated highway. The group apparently discovered that the automated vehicles were easy targets for roadside jamming. Without protection and appropriate back-up systems, communications were jammed between the lead vehicle (in a platoon of five) and the roadside sensors. Losing control, the lead vehicle caused a chain-reaction collision. Fortunately, no drivers or passengers were injured, but the automated highway has been closed pending further investigation by both the State and the system developer.

User services are designed to achieve ITS goals and objectives -- goals and objectives that will be achieved to a significant extent by maintaining information security. Had the systems described in these hypothetical events employed appropriate information security services and exercised proper information security management, such unfortunate consequences would have been avoided.

Due to the rapid evolution of information technologies, no security solution will be permanent. However, it is essential to develop a foundation on which further enhancements in ITS security can be developed.

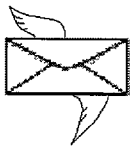
What can we do about it?

As the previous events illustrate, accidents, incorrect operations, and other unforeseen results can occur when ITS information -- or the information resources on which it is processed, stored, or transmitted -- is not adequately protected. The introduction of information technologies includes an associated level of risk, but specific security features can be incorporated into a system to mitigate that risk. What follows is a brief discussion of "security services" that can counter the major threats to automated information systems and a program plan to pull these security services together.

Technical Security Services

First, there are several **technical security services.** These services are provided by commercially available security mechanisms that can be integrated into computer and communications systems. These services can (and usually should) be transparent to users; however, users should be aware that security services are actually being provided. The most commonly used technical security services are described below.

Confidentiality helps restrict sensitive information from disclosure. Confidentiality applies to both information storage and transmission.

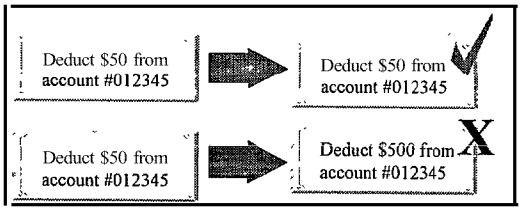


A common confidentiality mechanism is **encryption.** If the names, social security numbers, and credit ratings that the Carport County couple accessed had been encrypted, they would not have been able to understand, let alone steal, the information.

Authentication verifies one's identity or membership in a group.

An ATM user, for example, must have an ATM card and enter a **password** known as a PIN. While a common word used as a password can be easily guessed, a more complex phrase or a personal characteristic (e.g., a finger print) may be more difficult to break or "fake." Stronger authentication, for example, would have prevented the teenage hackers from breaking into the traffic management system.

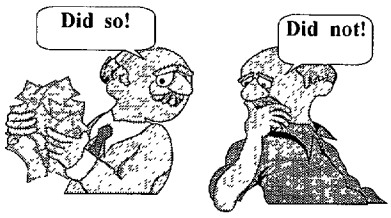
Data integrity ensures that information is not modified while stored or transmitted except by authorized users.



Automated methods like **digital signatures, cryptographic checksums,** and **automated range checks (e.g.,** month not equal to 13) can be used to indicate whether any information has changed during storage or transmission.

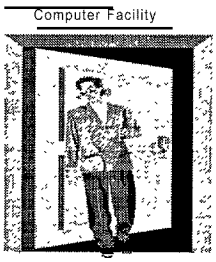
Without appropriate data integrity features on E911 transmissions, an emergency message indicating an accident could be modified and lead response crews to the wrong location.

Non-repudiation prohibits the sender or receiver of a transaction from subsequently denying the action.



A dishonest businessman who receives a customer payment may deny receiving it on time and subsequently charge a late fee. However, a payment **receipt** or a canceled check can easily counter this claim. In automated systems, **activity logs, electronic acknowledgments,** and **digital signatures** are often used to provide this service. Most emergency management systems record E911 calls in an effort to counter any accusations that staff did not respond -- or did not respond appropriately -- to the calls received.

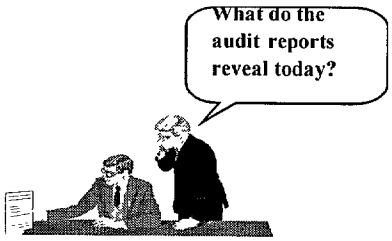
Access control regulates who can access a specific resource (e.g., information, applications, systems, or networks) and what they can do with that resource (e.g., read, write, execute).



If the Carport County couple had been required to provide additional **identification and authentication** information (e.g., an additional access code), they would not have been allowed to access the ISP server -- let alone the traveler information.

The concept of least privilege (an important aspect of access control) provides users only those access privileges that they need to perform their functions -- and nothing more. If the Redmont County clerk's access privileges had limited her to only the DMV's files and programs, she would not have been able to access the toll-tag data.

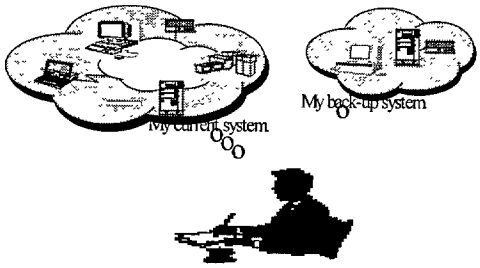
Accountability attributes actions to the users who perform them.



Information systems often use an audit mechanism to log users' activities (e.g., login, program execution) and the information-system resources that they used (e.g., processing time, computer memory). Audit analysis tools are then used to check for unusual or unauthorized activities, to summarize resource usage for planning and chargeback purposes, and to reconstruct events.

Audits of the traffic management system used to control the electronic-message signs might have revealed an unusually large number of failed login attempts. Audit entries of this type often indicate that an unauthorized user may be trying to access the system. Such activity would have alerted the system administrator that the system was being compromised,

Availability ensures that expected resources are available for their intended use and perform as expected.

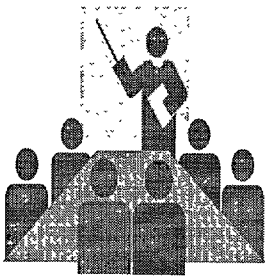


In information systems, availability applies to all system resources (e.g., data, software, printers, networks). Availability is often ensured by using redundant systems and communications pathways (e.g., a backup computer system that can be used if the main computer becomes inoperable) and system or process designs that address various conditions of operation. A manual override capability for the Slobovian computer might have halted the continuous submission of system requests to the main computer and prevented the shut-down of trains. Alternatively, a system design that separates the call-receiving functions from the dispatching functions might have prevented the EMS's unavailability.

Non-technical Security Services

There are three major **"non-technical security services"** that are required to support the technical security services implemented on information systems.

Administrative Security recognizes the need for managing information security throughout the organization. This includes establishment and operation of the proper administrative organizations and positions.

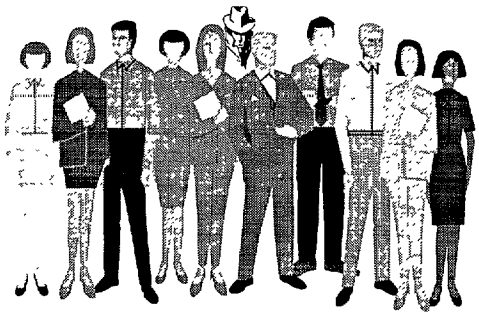


It also includes obtaining and managing the personnel and other resources required to manage and protect the organization's information resources.

The organization must establish, enforce, and review its **security policies and procedures.** During this process, emphasis should be placed on personnel security training, importing and exporting information to and from other organizations, handling security violations (e.g., suspending or prosecuting violators), and **strategic planning** of the organization's information security needs. The strategic plan must be reviewed and updated as the organization's functions and development objectives change.

Administrative security also includes requiring and assuring that "everyday" operations are completed in compliance with the organization's security policies. Everyday operations include, but are not limited to, assigning, changing and removing user IDs, passwords and network addresses, and making backup copies of the organization's data and software.

Personnel Security assures that employees, both local and remote to the information systems that they access, can be trusted in ways appropriate to their responsibilities.



Some staff, for example, may require pre-employment **screenings** and **special clearances** to use the information related to their positions; all employees may require **special identification badges** to access specific off-ices, vehicles, or computers. If the Redmont County clerk's identification badge had indicated that she was not allowed to access the DMV's Expressway Management computer facility, she might have been prevented from masquerading as a legitimate Expressway user.

Personnel security also encompasses **training** personnel (e.g., specific duties, emergency operations, cross training among staff, and security awareness). Perhaps more detailed training in the operation of the Slobovian traffic control system could have better assured the absence of small objects, including paper clips, from the computer workspace.

Physical Security is concerned with protecting the organization's personnel as well as its buildings, offices, equipment, and products from harm, destruction, and unauthorized access.

Safes can protect sensitive information (e.g., trade secrets, marketing strategies) from fire and flood damage as well as from access by those not authorized to **see** it. Door **locks** and **alarms** can protect employees and equipment from trespassers and potential burglars. Air conditioning and heating systems can provide the proper **operating environment** for the computer equipment as well as the personnel who operate it.

Physical security also includes developing, testing, and executing the plans and procedures for **recovering from disasters** -- geographic, weather-related, or political -- to which the organization's personnel and assets may be exposed.

Information Security Program

An information security program ties together all of the technical and non-technical components. Keep in mind that there are various methods for implementing a security program. Private companies may have their own versions and individual government agencies may have their own as well. The key point is to develop and follow a well-conceived, thorough security program that is appropriate for a particular environment and its associated threats.

An information security program can be viewed as a set of **fundamental information security activities.** These are activities that involve the technical and non-technical security services and that are applied to the system throughout its life-cycle. Regardless of the specific information security program developed, there are a few key points to first consider:

- Designate a central point of contact (an individual or team) for the information security program
- Obtain "buy-in" (i.e., acceptance, concurrence) from the major players such as acquisition managers, development teams, end-users, and other stake-holders
- Focus on the entire system, not just database security or physical security

The model described below presents a framework that can be modified as needed to fit the individual program office needs. It consists of six information security activities:

> **Strategic Security Planning**

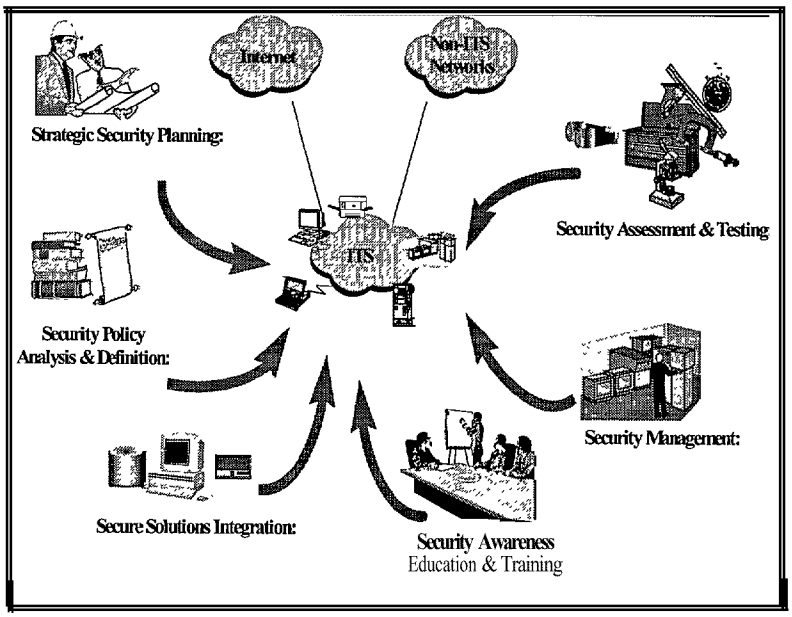
> **Security Policy Analysis & Definition**

> **Secure Solutions Integration**

> **Security Awareness, Education & Training**

> **Security Management**

> **Security Assessment & Testing**

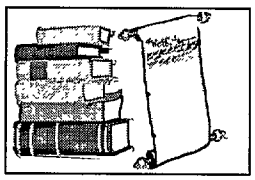


Strategic Security Planning occurs in the early stages of concept formulation and parallels other system engineering efforts. The purpose is to ensure that security is addressed in a systematic approach and is consistent with the objectives and mission on the ITS organization.

NIST Special Publication 800-4 provides guidance on incorporating information security requirements during the acquisition phase. Although this document is directed towards Federal information systems, it can be used as a guide for non-federal information systems (e.g., state-operated traffic management systems, private ITS information service providers).

One of the major planning activities involves conducting an **initial risk analysis.** The analysis is used to determine **potential threats** and **the initial security requirements** as well as the **costs/benefits** of any required security mechanisms.

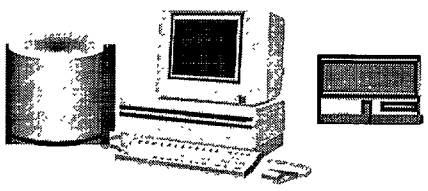
Security Policy Analysis and Definitions identify the rules to ensure that the security objectives (i.e., confidentiality, integrity, and availability) are met. Specifically, security policies identify the conditions under which data access, storage, and transmission will operate.



Security policies must take into account applicable legislative, regulatory, ethical, and organizational requirements (e.g., OMB A-130, Public Law 100-235, and the Privacy Act of 1974).

ITS will be implemented by state and local governments as well as by privately owned companies, and policy will most likely be derived from state, local or private **Information Resources Management (IRM) plans** or similar plans. Specific security requirements are then derived from the higher-level policy statements. The details of implementing security requirements are considered in the next activity.

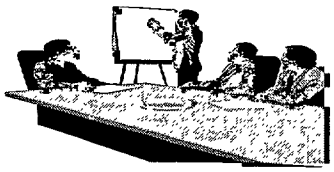
Secure Solutions Integration requires applying the appropriate combination of technical and non-technical security services to the system for a cost-effective, robust yet user-friendly, and effective interoperable solution (i.e., design). That is, the "whole is greater than the sum of its parts."



A tenable business case must be made for any engineered solutions -- including those for security. A secure solution takes into account new and legacy systems, existing and missing infrastructures, secure and non-secure products and protocols, consumer expectations, as well as the costs and benefits of these factors.

Such a comprehensive solution could require using **identical authentication mechanisms and procedures** at computer facilities; using **compatible cryptographic technologies** for the various service payment schemes; and installing firewalls that support authentication schemes already in use with ITS systems.

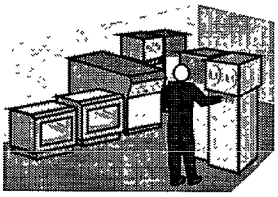
Security Awareness, Education & Training is a process for informing users of threats to the systems, the measures to protect the systems from those threats, and the proper security procedures for implementing and maintaining the protection measures.



As new technologies are incorporated into ITS, education an training will be necessary for maintaining the security posture of the system. This activity will ensure that users and administrators are aware of the importance of protecting system data and resources. Likewise, a complete security **training program** (e.g., seminars, announcements, demos, pamphlets} will ensure that employees are trained in the use of security tools and products. It will also ensure that they are aware of security policies and procedures.

A well-engineered security solution is only as good as its design and the individuals operating and maintaining it.

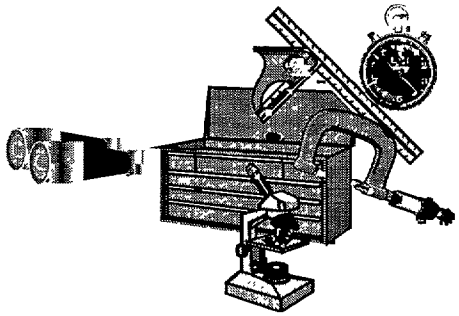
Security Management can be viewed as an extension of the **previous education** and training activity. It is a continual administrative security activity that incorporates procedural and technical security features. Management procedures should be reviewed periodically and updated as needed. By doing so, system security is maintained should a contingency arise.



The most advanced security tools and technologies are only as effective as the ways in which they are managed. If simple security mechanisms (e.g., user accounts) are not properly managed, even the most sophisticated authentication technique may offer little or no protection.

Some appropriate **security management responsibilities for ITS subsystems may include:** operating system security, software and hardware configuration management, data and software integrity verification, audit log inspection, periodic risk assessments, and contingency plan and procedure development.

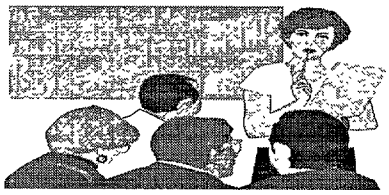
Security Assessment and Testing are performed in the later stages of system development or system operation, or after any system modification, upgrade, or change in connectivity.



These activities entail **assessments of the system security posture and** range from **high-level paper analysis to specific penetration tests** of varying degrees of aggression. The results of assessments and testing provide system administrators and managers with a "security health diagnosis" of the system, Assessments are good indicators as to how well security procedures are being followed. Alternatively, testing provides direct feedback on the technical security mechanisms employed. Independent auditors, analysis teams, and test agents are typically used to assess a system and thus provide unbiased test results. The tools used in the testing process can include both public and propriety programs. Furthermore, in-house testing can be used in conjunction with independent testing to validate risk assessment conclusions.

Frequently Asked Questions (FAQ)

Although many security issues have been addressed in the previous sections, the following questions represent a broad range of additional management-level concerns.



Q: Why should I have information security?

Information security helps an organization accomplish its mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets. However, information security is often viewed as hampering the mission by imposing unrealistic restrictions on systems, managers, operators, and users. Implementing information security is too often a reactive maneuver that follows an embarrassing incident. Superior information security is achieved by early planning.

Q: What if I do not incorporate information security?

The potential impacts should be apparent from the hypothetical events depicted earlier in this document. However, one can easily envision **various adverse consequences based on the particular ITS services being provided, managed, operated, or used.** These might include the inability to perform intended functions and provide required services (both critical and trivial); the waste, loss, misuse, or misappropriation of funds; compromise of citizen privacy or public safety; the potential for legal and safety liabilities; and the loss of organizational credibility.

Q: What is the ITS community doing about information security?

Adequately protecting information from various threats is only slowly being realized within the surface transportation community. Through ITS America, the industry has pursued privacy issues by developing a set of **"Fair Information and Privacy Principles".** While not specifically addressing information security, these principles do recognize the importance of protecting individual privacy within ITS. Additionally, some of the more recent activities include the ***ITS Information Security*** Analysis conducted by Mitretek Systems for the ITS Joint Program Office (JPO) and the President's Commission on Critical Infrastructure Protection (PCCIP); **the** ***Maryland ITS Security Requirements Recommendations*** and ***Maryland ITS Security Implementation Recommendations*** conducted by Computer Sciences Corporation for Volpe National Transportation Systems Center (NTSC); and ***this awareness document.***

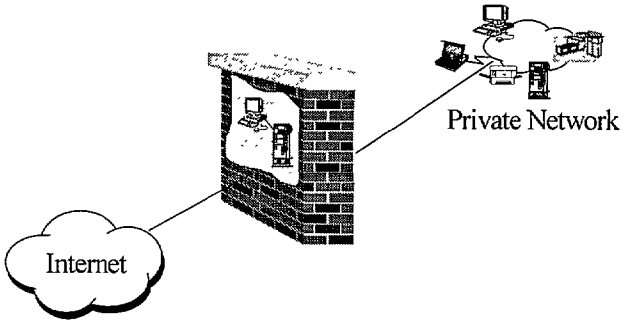
Q: When do we address information security?

Information security should be addressed **throughout the life-cycle process.** However, providing automated protection using a secure system as the basic building block should always be considered during the system acquisition phase. Frequently, information security has been neglected during system acquisition. Only when a serious mishap occurs (e.g., the misuse of financial information) do implementors attempt to retrofit a system with the necessary information security mechanisms. Therefore, if secure solutions are addressed during system acquisition, the potential needs and costs to re-engineer or retrofit a security solution are minimized.

Toward this goal, NIST provides some procurement guidelines (e.g., NIST, Special Publication *800-4, Computer Security Considerations In Federal Procurements)* for incorporating information security during the system acquisition phase.

Q: Firewalls seem to be a "hot topic" in information security. What are they and what do they do?

A **firewall** is a collection of hardware and software components placed between networks to protect one network from another (e.g., a private network from the Internet). It is important to remember that a firewall is not the end-all solution; rather, it should be used in conjunction with other information security mechanisms. That is, firewalls provide *access control* to an organization's internal network; *confidentiality, integrity,* and *authentication* must be provided by other security mechanisms.



Other "hot topics" or "buzzwords" include:

Encryption -- the process of disguising data such that it cannot be read unless the data is decrypted. Depending upon the specific technique, encryption can also be used to provide authentication, integrity, and non-repudiation in addition to the traditional use of providing confidentiality.

Digital signature -- a security mechanism that is the electronic equivalent of a hand-written signature and can be attached to electronic transactions. The primary purpose of a digital signature is to provide non-repudiation; however, authentication and integrity are provided by this mechanism as well.

Privacy -- protecting personal information from unauthorized collection, use, storage, and dissemination.

Q: Why is there often confusion regarding security terminologies?

Different organizations with different origins define information security concepts differently. Even the leading security experts in the world do not all agree on definitions and groupings. Some describe threats differently; some describe technical and non-technical security services differently (if they call them security "services"); some have different terminologies and content for what we have termed "security management, security planning, security policy, and solution integration". Why? Good question.

This is not a trivial matter when trying to establish good information security, but the fact is that the industry is not consistent. Often, organizations are describing technologies and processes that provide similar results, but the **terminology confusion may cause apparent conflicts between potential guidelines, policies, and practices (e.g., State IRMs, DOT guidelines) or various system design requirements.**

The solution is to adapt as well as possible to the various models and terminologies that best suit the particular activity. The definitions used in this document represent an attempt to be consistent with the industry's state of the practice. However, find another information security text, and you will probably find some apparent discrepancies!

Q: What are the costs, risks, and benefits of information security?

Costs: Information security incurs **direct and indirect costs.** Direct costs are incurred for purchasing, installing, and administering security measures. Additionally, security measures sometimes affect system performance, employee morale, or retraining requirements. Such indirect costs must be considered in addition to the basic cost of the control itself. These additional costs may well exceed the direct cost of the control (as is often seen, for example, in the costs of administering an access control package).

Several studies have shown that the **costs of incorporating requirements (e.g., security requirements) increase at an exponential rate as the system develops through the operations and maintenance (O&M) stage.** Costs to add a system requirement during the O&M stage can be close to 100% greater than if added during the initial requirements stage (Davis, Alan M., *Software Requirements Objects, Functions, and States).* **Solutions to security problems should not be chosen if they cost more (in monetary or non-monetary terms, directly or indirectly) than simply tolerating the problem** (NIST, *Generally Accepted Principles).*

Risks: Cost-effective security results when risk reduction is balanced with costs. The greater the value of information processed, or the more severe the consequences if something happens to that information, the greater the need for control measures to protect it. What will the impacts be if the data is inaccurate or unavailable? It is important that trade-offs of cost versus risk reduction be explicitly considered and that management understand the degree of risk remaining after selected controls are implemented (NIST, *Management Guide to the Protection of Information Resources).*

Benefits: In general, information security is a smart business practice. Just **a few of its benefits include consumer confidence, increased use, reduced recovery, and lower information maintenance.** By investing in security measures, an organization can reduce the frequency and severity of information security-related losses. For example, an organization may estimate that it is experiencing significant losses in inventory through fraudulent manipulation of its systems. Security services, such as access control, may significantly reduce the loss (NIST, *Generally Accepted Principles).* Furthermore, access control implemented via secure operating procedures or other administrative controls may prove to be more cost effective than a technical access control solution.

The costs and benefits of security should be carefully examined in both monetary and non-monetary terms to **ensure that the cost of controls does not exceed expected benefits.**

Q: What are the appropriate amounts of information security?

The appropriate amount(s) of security will vary, but no matter what is used, one will most likely never achieve total security. One can, however, decrease risks in proportion to the strength of the protective measures used. As determined by appropriate cost vs. risk and cost vs. benefit assessments, **the level of security is based on the value of the information.** How serious would the consequences be if a certain type of information were to be wrongfully manipulated, disclosed, reused, or delayed (NIST, *User's Guide)?*

Q: What is sensitive data?

Sensitive data is any data that is worth protecting. The exact sensitivity and precise protections are unique to each business environment. Within ITS, there will be varying levels of sensitive information; examples include: law enforcement (e.g., violations), financial (e.g., a traveler's credit card number), personal privacy (e.g., a traveler's itinerary). One way to determine the sensitivity of data is to ask the questions "What will it cost if the data is wrong? manipulated for fraudulent purposes? not available? given to the wrong person?" If the damage is more than can be tolerated, then the data is sensitive and should have adequate security controls to prevent or lessen the potential loss (NIST, *User's Guide).*

Q: Are we required to employ information security measures?

ITS will be implemented by state and local governments as well as by privately owned companies; therefore, **policies and practices will most likely be derived from state/local government or private corporation Information Resource Management (IRM) plans** (or similar documents). Although most state and local governments have official policies on information security, it is likely that these policies deal only with internal computer issues and do not deal with external systems and communication networks such as those used in ITS applications.

A comprehensive and contemporary IRM plan has been produced by the state of Texas. This plan is intended to assist in the implementation of an adequate security program to protect the automated information resources within the various agencies of the Texas state government (including transportation). The security standards and policy are required procedures and controls to be implemented as part of any Texas government agency's information security program. The optional guidelines are meant to assist agencies in the interpretation and implementation of the standards and are recommended as effective security practices. Each state agency is encouraged to evaluate the policy, standards, and guidelines to determine whether more stringent requirements are necessary given the individual agency's authority and function.

Q: What about private sector entities collaborating on projects?

The content of security policies and their enforcement practices in the private sector cover a broad spectrum. Security policies have various degrees of enforcement. At the weaker end, companies that do have a security policy do not always enforce it or keep it current and are often susceptible to various threats. Companies with stronger security enforcement use either a combination of internal security protections (e.g., strict access control) and external protections (e.g., firewalls) -- a proactive approach; or they implement stringent auditing of user activity -- a reactive approach.

Because many information infrastructure components are owned and operated by the private sector, **it is essential that the Government and private sector work together to develop a strategy for protecting these components and ensuring their continued operation.** In the case of transportation, there is no regulatory mandate for a Federal agency such as the USDOT to intervene or to direct private companies to take specific security precautions, nor is there any requirement for the USDOT to react in the case of an attempt at unauthorized access to a private transportation system. However, the Federal government can promote awareness among the private sector by making private companies aware of the potential vulnerabilities and costs of such incidents and the advantages of taking prudent precautions.

The Economic Espionage Act of 1996 punishes the theft, modification, or destruction of commercial trade secrets via traditional (physical) and non-traditional (i.e., electronic) means. The Act applies to both attempted and successful actions against both Federal and non-Federal systems.

Where do we get more information?

This document is not intended to provide a comprehensive lesson on information security or its relation to surface transportation. However, there are several resources available to help initiate, update, and/or modify a transportation agency's information security policies, practices, or procedures.

The following may provide this support.

ITS Information Security Documents

Intelligent Transportation Systems (ITS) Information Security Analysis, Mitretek Systems, 1997. (contact William S. Jones, ITS JPO)

> This document presents the results from an information security analysis of the National ITS Architecture. The ITS information security analysis comprises three assessments to identify and characterize the various threats to (1) the ITS subsystems, (2) their exchange of information, and (3) their supporting communications infrastructure. The assessments also recommend solutions (i.e., security services) that can be used to reduce or eliminate identified threats and to better protect ITS.
>
> This analysis was conducted jointly for the Presidential Commission on Critical Infrastructure Protection (PCCIP) and the ITS Joint Program Office (JPO).

Maryland ITS Security Requirements Recommendations and ***Ma yland ITS Security Implementation Recommendations,*** Computer Sciences Corporation for Volpe National Transportation Systems Center (NTSC), 1997. (contact William S. Jones, ITS JPO)

> These studies are a follow-on to the Mitretek ***ITS Information Security Analysis.*** They recommend implementation of security guidelines for Maryland ITS and include reviewing the State's planned development cycle. They also describe steps necessary to achieve a minimal level of security for Maryland ITS.

Information Resource Documents

Information Resources Security and Risk Management, Texas Department of Information Resources

Information Technology Security and Risk Management Guidelines, California Office of Information Technology

Each exemplifies methods for establishing and maintaining acceptable levels of security.

National Institute of Standards and Technology (NIST)

For further information on the management of information resources, NIST publishes Federal Information Processing Standards Publications (FIPS PUB).

The following NIST special publications are referenced in this paper:

- SP 500-170, *Management Guide to the Protection of information Resources,* 1989.
- SP 500-l71, *Computer Users' Guide to the Protection of Information Resources,* 1989.
- SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems,* 1995.
- SP 800-4, *Computer Security Considerations in Federal Procurements.. A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials, 1992.*

These documents and other related information are currently available from NIST's Computer Security Resource Clearinghouse at http://csrc.ncsl.nist.gov.

Commissions, Committees, Institutes, and Councils

President's Commission on Critical Infrastructure Protection (PCCIP)

This Commission was created by executive order in July 1996 to recommend a national strategy for protecting critical infrastructures (including transportation). The Commission's Web site is at http://www.pccip.gov.

National Security Telecommunications Advisory Committee (NSTAC) Information Infrastructure Group (IIG)

The NSTAC utilizes its Information Infrastructure Group to serve as the focal point for assessing information assurance threats to, and the vulnerabilities of, the information or communications components that control critical infrastructures (including transportation). Some additional NSTAC information may be found at http://www.ncs.gov/nstac.htm.

International Institute for Surface Transportation Policy Studies (IISTPS)

Established at San Jose State University as part of the Intermodal Surface Transportation Efficiency Act of 199 1 (ISTEA), this organization focuses on international surface transportation policy issues related to three primary responsibilities: research, education, and information transfer. This group has begun to address some aspects of security (e.g., physical, procedural) on current transportation systems. The Institute's Web site is at http://transweb.sjsu.edu/

The National Science and Technology Council (NSTC)

The NSTC's Transportation Research and Development Committee is currently investigating information security within the transportation domain. The Council's Web site is found through http://www.whitehouse.gov.

Who can we contact?

United States Department of Transportation (USDOT), Intelligent Transportation Systems (ITS) Joint Program Office (JPO)

William S. Jones, Technical Director
(202) 366-2128
william.s.jones@fhwa.dot.gov

http://www.its.dot.gov/program/jpobios2.htm

(publication number: FHWA-JPO-98-005)
HVH-1 \ 11-97